Amendments to the Claims:

This listing of claims will replace all prior version, and listings, of claims in the application. Where claims have been amended and/or canceled, such amendments and/or cancellations are done without prejudice and/or waiver and/or disclaimer to the claimed and/or disclosed subject matter, and the applicant and/or assignee reserves the right to claim this subject matter and/or other disclosed subject matter in a continuing application.

Listing of the claims:

Claim 1 - Claim 86 (Canceled)

Claim 87 (Currently Amended) A method for protecting decrypted digital data from illegitimate use, ~~said decrypted digital data being decrypted from enerypted digital data,~~ said method comprising:

encrypting said decrypted digital data using a changeable key to produce changeable key re-encrypted digital data;

encrypting said changeable key re-encrypted digital data using an unchangeable key to produce changeable-unchangeable keys double re-encrypted digital data to be stored, copied and/or transferred, wherein said unchangeable key is capable of being operationally unchangeable at least during said encrypting of said changeable key re-encrypted digital data;

decrypting said copied, stored and/or transferred changeable-unchangeable keys double re-encrypted digital data using said unchangeable key to said changeable key re-encrypted digital data; and

decrypting said changeable key re-encrypted digital data using said changeable key to said decrypted digital data.

Claim 88 (Currently Amended) The method of claim 87 wherein said unchangeable key is located ~~may be~~ in a device.

Claim 89 (Currently Amended) A method for protecting decrypted digital data from illegitimate use, ~~said decrypted digital data being decrypted from encrypted digital data,~~ comprising:

encrypting said decrypted digital data using an unchangeable key to produce unchangeable key re-encrypted digital data, wherein said unchangeable key is capable of being operationally unchangeable at least during said encrypting of said decrypted digital data;

encrypting said unchangeable key re-encrypted digital data using a changeable key to produce unchangeable-changeable key double re-encrypted digital data to be stored, copied and/or transferred;

decrypting said copied, stored and/or transferred unchangeable-changeable keys double re-encrypted digital data using said changeable key to said unchangeable key re-encrypted digital data; and

decrypting said unchangeable key re-encrypted digital data using said unchangeable key to said decrypted digital data.

Claim 90 (Currently Amended) The method of claim 89 wherein said unchangeable key is located ~~may be~~ in a device.

Claim 91 (Currently Amended) The method according to claim 87 or 89, wherein said encrypting and decrypting using said changeable key are carried out by [[a]] software executed by a computer.

Claim 92 (Currently Amended) The method according to claim 87 or 89, wherein said encrypting and decrypting using said changeable key are carried out by [[a]] hardware.

Claim 93 (Previously Presented) The method according to claim 88 or 90, wherein said changeable key is supplied externally from said device.

Claim 94 (Previously Presented) The method according to claim 88 or 90, wherein said changeable key is generated in said device.

Claim 95 (Currently Amended) The method according to claim 88 or 90, wherein said encrypting and decrypting using said unchangeable key are carried out by [[a]] software executed by a computer.

Claim 96 (Currently Amended) The method according to claim 87 or 89, wherein said encrypting and decrypting using said unchangeable key are carried out by [[a]] hardware.

Claim 97 (Previously Presented) The method according to claim 88 or 90, wherein said unchangeable key is already placed in said device.

Claim 98 (Previously Presented) The method according to claim 88 or 90, wherein said unchangeable key is generated in said device.

Claim 99 (Previously Presented) The method according to claim 88 or 90, wherein said unchangeable key is supplied externally from said device.

Claim 100 (Previously Presented) The method according to claim 88 or 90, wherein said unchangeable key is specific to said device.

Claim 101 (Previously Presented) The method according to claim 88 or 90 wherein said unchangeable key is not specific to said device.

Claim 102 (Currently Amended) An apparatus for protecting decrypted digital data from illegitimate use, ~~said decrypted digital data being decrypted from encrypted digital data,~~ said apparatus comprising:

a changeable key encryption unit capable of ~~for~~ encrypting said decrypted digital data using a changeable key to produce changeable key re-encrypted digital data;

an unchangeable key encryption unit capable of ~~for~~ encrypting said changeable key re-encrypted digital data using an unchangeable key to produce changeable-unchangeable keys double re-encrypted digital data to be stored, copied and/or

transferred, wherein said unchangeable key is capable of being operationally unchangeable at least during production of said changeable-unchangeable keys double re-encrypted digital data;

an unchangeable key decryption unit capable of ~~for~~ decrypting said copied, stored and/or transferred changeable-unchangeable keys double re-encrypted digital data using said unchangeable key to said changeable key re-encrypted digital data; and

a changeable key decryption unit capable of ~~for~~ decrypting said changeable key re-encrypted digital data using said changeable key to said decrypted digital data.

Claim 103 (Currently Amended) The apparatus of claim 102 wherein said unchangeable key is located ~~may be~~ in a device.

Claim 104 (Currently Amended) An apparatus for protecting decrypted digital data from illegitimate use, ~~said decrypted digital data being decrypted from enerypted digital data,~~ said apparatus comprising:

an unchangeable key encryption unit capable of ~~for~~ encrypting said decrypted digital data using an unchangeable key to produce unchangeable key re-encrypted digital data, wherein said unchangeable key is capable of being operationally unchangeable at least during production of said unchangeable key re-encrypted digital data;

a changeable key encryption unit capable of ~~for~~ encrypting said unchangeable key re-encrypted digital data using a changeable key to produce changeable-unchangeable keys double re-encrypted digital data to be stored, copied and/or transferred;

a changeable key decryption unit capable of ~~for~~ decrypting said copied, stored and/or transferred
changeable-unchangeable keys double re-encrypted digital data using said changeable key to said unchangeable key re-encrypted digital data; and

an unchangeable key decryption unit capable of ~~for~~ decrypting said unchangeable key re-encrypted digital data using said unchangeable key to said decrypted digital data.

Claim 105 (Currently Amended) The apparatus of claim 104 wherein said unchangeable key is located ~~may be~~ in a device.

Claim 106 (Currently Amended) The apparatus according to claim 102 or 104, in which encrypting and decrypting using said changeable key are carried out by [[a]] software executed by a computer.

Claim 107 (Currently Amended) The apparatus according to claim 102 or 104, in which encrypting and decrypting using said changeable key are carried out by [[a]] hardware.

Claim 108 (Previously Presented) The apparatus according to claim 103 or 105, wherein said changeable key is supplied externally from said device.

Claim 109 (Previously Presented) The apparatus according to claim 103 or 105, wherein said changeable key is generated in said device.

Claim 110 (Currently Amended) The apparatus according to claim 102 or 104, in which encrypting and decrypting using said unchangeable key are carried out by [[a]] software executed by a computer.

Claim 111 (Currently Amended) The apparatus according to claim 102 or 104, in which encrypting and decrypting using said unchangeable key are carried out by [[a]] hardware.

Claim 112 (Previously Presented) The apparatus according to claim 103 or 105, wherein said unchangeable key is already placed in said device.

Claim 113 (Previously Presented) The apparatus according to claim 103 or 105, wherein said unchangeable key is generated in said device.

Claim 114 (Previously Presented) The apparatus according to claim 103 or 105, wherein said unchangeable key is supplied externally from said device.

Claim 115 (Previously Presented) The apparatus according to claim 103 or 105, wherein said unchangeable key is specific to said device.

Claim 116 (Previously Presented) The apparatus according to claim 103 or 105, wherein said unchangeable key is not specific to said device.

Claim 117 (Currently Amended) A method for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said method comprising:

encrypting said decrypted digital data using a second changeable key to produce second changeable key re-encrypted digital data;

encrypting said second changeable key re-encrypted digital data using an unchangeable key to produce unchangeable second changeable keys double re-encrypted digital data to be stored, wherein said unchangeable key is capable of being operationally unchangeable at least during said encrypting of said second changeable key re-encrypted digital data;

decrypting said stored unchangeable-second changeable keys double re-encrypted digital data using said unchangeable key to said second changeable key re-encrypted digital data;

encrypting said second changeable key re-encrypted digital data using a third changeable key to produce third changeable-second changeable keys double re-encrypted digital data to be copied and/or transferred;

decrypting said copied and/or transferred third changeable-second changeable keys double re-encrypted digital data using said third changeable key to said second changeable key re-encrypted digital data; and

decrypting said second changeable key re-encrypted digital data using said second changeable key to said decrypted digital data.

Claim 118 (Currently Amended) The method of claim 117 wherein said unchangeable key is located ~~may be~~ in a device.

Claim 119 (Currently Amended) A method for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said method comprising:

encrypting said decrypted digital data using an unchangeable key to produce unchangeable key re-encrypted digital data, wherein said unchangeable key is capable of being operationally unchangeable at least during said encrypting of said decrypted digital data, and encrypting said unchangeable key re-encrypted digital data using a second changeable key to produce second changeable-unchangeable keys double re-encrypted digital data to be stored;

decrypting said stored second changeable-unchangeable keys double re-encrypted digital data using said second changeable key to said unchangeable key re-encrypted digital data;

decrypting said unchangeable key re-encrypted digital data using said unchangeable key to said decrypted digital data;

encrypting said decrypted digital data using a third changeable key to produce third changeable key re-encrypted digital data, and encrypting said third changeable key re-encrypted digital data using said second changeable key to produce second changeable-third changeable keys double re-encrypted digital data to be copied and/or transferred;

decrypting said copied and/or transferred second changeable-third changeable keys double re-encrypted digital data using said second changeable key to said third changeable key re-encrypted digital data; and

decrypting said third changeable key re-encrypted digital data using said third changeable key to said decrypted digital data.

Claim 120 (Currently Amended) The method of claim 119 wherein said unchangeable key is located ~~may be~~ in a device.

Claim 121 (Currently Amended) The method according to claim 117 or 119 wherein said encrypting and decrypting using said second changeable key are carried out by [[a]] software executed by a computer.

Claim 122 (Currently Amended) The method according to claim 117 or 119 wherein said encrypting and decrypting using said second changeable key are carried out by [[a]] hardware.

Claim 123 (Previously Presented) The method according to claim 118 or 120 wherein said second changeable key is supplied externally from said device.

Claim 124 (Previously Presented) The method according to claim 118 or 120 wherein said second changeable key is generated in said device.

Claim 125 (Currently Amended) The method according to claim 117 or 119 wherein said encrypting and decrypting using said third changeable key are carried out by [[a]] software executed by a computer.

Claim 126 (Currently Amended) The method according to claim 117 or 119 wherein said encrypting and decrypting using said third changeable key are carried out by [[a]] hardware.

Claim 127 (Previously Presented) The method according to claim 118 or 120 wherein said third changeable key is supplied externally from said device.

Claim 128 (Previously Presented) The method according to claim 118 or 120 wherein said third changeable key is generated in said device.

Claim 129 (Currently Amended) The method according to claim 117 or 119 wherein said encrypting and decrypting using said unchangeable key are carried out by [[a]] software executed by a computer.

Claim 130 (Currently Amended) The method according to claim 117 or 119 wherein said encrypting and decrypting using said unchangeable key are carried out by [[a]] hardware.

Claim 131 (Previously Presented) The method according to claim 118 or 120 wherein said unchangeable key is already placed in said device.

Claim 132 (Previously Presented) The method according to claim 118 or 120 wherein said unchangeable key is generated in said device.

Claim 133 (Previously Presented) The method according to claim 118 or 120 wherein said unchangeable key is supplied externally from said device.

Claim 134 (Previously Presented) The method according to claim 118 or 120 wherein said unchangeable key is specific to said device.

Claim 135 (Previously Presented) The method according to claim 118 or 120 wherein said unchangeable key is not specific to said device.

Claim 136 (Currently Amended) An apparatus for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said apparatus comprising:

a second changeable key encryption unit capable of ~~for~~ encrypting said decrypted digital data using a second changeable key to produce second changeable key re-encrypted digital data;

an unchangeable key encryption unit capable of ~~for~~ encrypting said second changeable key re-encrypted digital data using an unchangeable key to produce unchangeable-second changeable keys double re-encrypted digital data to be stored, wherein said unchangeable key is capable of being operationally unchangeable at least during production of said unchangeable-second changeable keys double re-encrypted digital data;

an unchangeable key decryption unit capable of ~~for~~ decrypting said stored unchangeable-second changeable keys double re-encrypted digital data using said unchangeable key to said second changeable key re-encrypted digital data;

a third changeable key encryption unit capable of ~~for~~ encrypting said second changeable key re-encrypted digital data using a third changeable key to produce third changeable-second changeable keys double re-encrypted digital data to be copied and/or transferred;

a third changeable key decryption unit capable of ~~for~~ decrypting said copied and/or transferred changeable-second changeable keys double re-encrypted digital data using said third changeable key to said second changeable key re-encrypted digital data; and

a second changeable key decryption unit capable of ~~for~~ decrypting said second changeable key re-encrypted digital data using said second changeable key to decrypted digital data.

Claim 137 (Currently Amended) The apparatus of claim 136 wherein said unchangeable key is located ~~may be~~ in a device.

Claim 138 (Currently Amended) An apparatus for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said apparatus comprising:

an unchangeable key encryption unit capable of ~~for~~ encrypting said decrypted digital data using an unchangeable key to produce unchangeable key re-encrypted digital data, wherein said unchangeable key is capable of being operationally unchangeable at least during production of said unchangeable key re-encrypted digital data, and a second changeable key encryption unit capable of ~~for~~ encrypting said unchangeable key re-encrypted digital data using a second changeable key to produce second changeable-unchangeable key double re-encrypted digital data to be stored;

a second changeable key decryption unit capable of ~~for~~ decrypting said stored second changeable-unchangeable keys double re-encrypted digital data using said second changeable key to unchangeable key re-encrypted digital data, and an unchangeable key decryption unit capable of ~~for~~ decrypting said unchangeable key re-encrypted digital data using said unchangeable key to decrypted digital data;

a third changeable key encryption unit capable of encrypting said decrypted digital data using a third changeable key to produce third changeable key re-encrypted digital data, and a second changeable key encryption unit capable of ~~for~~ encrypting said third changeable key re-encrypted digital data using said second changeable key to produce second changeable-third changeable keys double re-encrypted digital data to be copied and/or transferred; and a second changeable key decryption unit capable of ~~for~~ decrypting said copied and/or transferred second changeable-third changeable keys double re-encrypted digital data using said second changeable key to said third changeable key re-encrypted digital data, and a third changeable key decryption unit capable of ~~for~~ decrypting said third changeable key re-encrypted digital data using said third changeable key to decrypted digital data.

Claim 139 (Currently Amended) The apparatus of claim 138 wherein said unchangeable key is located ~~may be~~ in a device.

Claim 140 (Currently Amended) The apparatus according to claim 136 or 138 wherein said encrypting and decrypting using said second changeable key are carried out by [[a]] software executed by a computer.

Claim 141 (Currently Amended) The apparatus according to claim 136 or 138 wherein said encrypting and decrypting using said second changeable key are carried out by [[a]] hardware.

Claim 142 (Previously Presented) The apparatus according to claim 137 or 139 wherein said second changeable key is supplied externally from said device.

Claim 143 (Previously Presented) The apparatus according to claim 137 or 139 wherein said second changeable key is generated in said device.

Claim 144 (Currently Amended) The apparatus according to claim 137 or 139 wherein said encrypting and decrypting using said third changeable key are carried out by [[a]] software executed by a computer.

Claim 145 (Currently Amended) The apparatus according to claim 136 or 138 wherein said encrypting and decrypting using said third changeable key are carried out by [[a]] hardware.

Claim 146 (Previously Presented) The apparatus according to claim 137 or 139 wherein said third changeable key is supplied externally from said device.

Claim 147 (Previously Presented) The apparatus according to claim 137 or 139 wherein said third changeable key is generated in said device.

Claim 148 (Currently Amended) The apparatus according to claim 136 or 138 wherein said encrypting and decrypting using said unchangeable key are carried out by [[a]] software executed by a computer.

Claim 149 (Currently Amended) The apparatus according to claim 136 or 138 wherein said encrypting and decrypting using said unchangeable key are carried out by [[a]] hardware.

Claim 150 (Previously Presented) The apparatus according to claim 137 or 139 wherein said unchangeable key is already placed in said device.

Claim 151 (Previously Presented) The apparatus according to claim 137 or 139 wherein said unchangeable key is generated in said device.

Claim 152 (Previously Presented) The apparatus according to claim 137 or 139 wherein said unchangeable key is supplied externally from said device.

Claim 153 (Previously Presented) The apparatus according to claim 137 or 139 wherein said unchangeable key is specific to said device.

Claim 154 (Previously Presented) The apparatus according to claim 137 or 139 wherein said unchangeable key is not specific to said device.

Claim 155 (Currently Amended) A method for protecting digital data from illegitimate use, said method comprising:

determining whether said digital data is subject to be protected or not;

encrypting said digital data, determined to be protected, using an unchangeable key to produce unchangeable key encrypted digital data, wherein said unchangeable key is capable of being operationally unchangeable at least during said encrypting of said digital data;

storing, copying and/or transferring said unchangeable key encrypted digital data;

decrypting said stored, copied and/or transferred unchangeable key encrypted digital data using said unchangeable key to decrypted digital data; and

utilizing said stored, copied and/or transferred unchangeable key encrypted digital data and said decrypted digital data.

Claim 156 (Currently Amended) The method of claim 155 wherein said unchangeable key is located ~~may be~~ in a device.

Claim 157 (Currently Amended) The method according to claim 155, wherein said encrypting and decrypting using said unchangeable key are carried out by [[a]] software executed by a computer.

Claim 158 (Currently Amended) The method according to claim 155, wherein said encrypting and decrypting using said unchangeable key are carried out by [[a]] hardware.

Claim 159 (Previously Presented) The method according to claim 155, in which encrypting and decrypting using said unchangeable key are controlled by identifying information which is added to said digital data.

Claim 160 (Currently Amended) The method according to claim 159, in which encrypting and decrypting are carried out [[when]] if said identifying information is present.

Claim 161 (Currently Amended) The method according to claim 159, in which encrypting and decrypting are carried out [[when]] if said identifying information is absent.

Claim 162 (Previously Presented) The method according to claim 156, wherein said unchangeable key is already placed in said device.

Claim 163 (Previously Presented) The method according to claim 156, wherein said unchangeable key is generated in said device.

Claim 164 (Previously Presented) The method according to claim 156, wherein said unchangeable key is supplied externally from said device.

Claim 165 (Previously Presented) The method according to claim 162, 163 or 164, wherein said unchangeable key is specific to said device.

Claim 166 (Previously Presented) The method according to claim 162, 163 or 164, wherein said unchangeable key is not specific to said device.

Claim 167 (Currently Amended) An apparatus for protecting digital data from illegitimate use, said apparatus comprising:

determining means for determining whether said digital data is subject to be protected or not;

means for encrypting said digital data, determined being subject to be protected, using an unchangeable key to produce unchangeable key encrypted digital data, wherein said unchangeable key is capable of being operationally unchangeable at least during said encrypting of said digital data;

means for storing, copying and/or transferring said unchangeable key encrypted digital data;

means for decrypting said stored, copied and/or transferred unchangeable key encrypted digital data to said decrypted digital data; and

means for utilizing said stored, copied and/or transferred unchangeable key encrypted digital data and said decrypted digital data.

Claim 168 (Currently Amended) The apparatus of claim 167 wherein said unchangeable key is located ~~may be~~ in a device.

Claim 169 (Currently Amended) The apparatus according to claim 167, wherein encrypting and decrypting using said unchangeable key are carried out by [[a]] software executed by a computer.

Claim 170 (Currently Amended) The apparatus according to claim 167, wherein encrypting and decrypting using said unchangeable key are carried out by [[a]] hardware.

Claim 171 (Previously Presented) The apparatus according to claim 167, wherein encrypting and decrypting using said unchangeable key are controlled by identifying information which is added to said digital data.

Claim 172 (Currently Amended) The apparatus according to claim 167, wherein encrypting and decrypting are carried out [[when]] if said identifying information is present.

Claim 173 (Currently Amended) The apparatus according to claim 167, wherein encrypting and decrypting are carried out [[when]] if said identifying information is absent.

Claim 174 (Previously Presented) The apparatus according to claim 168, wherein said unchangeable key is already placed in said device.

Claim 175 (Previously Presented) The apparatus according to claim 168, wherein said unchangeable key is generated in said device.

Claim 176 (Previously Presented) The apparatus according to claim 168, wherein said unchangeable key is supplied externally from said device.

Claim 177 (Previously Presented) The apparatus according to claim 174, 175 or 176 wherein said unchangeable key is specific to said device.

Claim 178 (Previously Presented) The apparatus according to claim 174, 175 or 176 wherein said unchangeable key is not specific to said device.